МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЄРЕВАНСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ

ЗАТВЕРДЖУЮ
Директор Єреванського навчально-наукового інституту ЗУНУ

_____ Саак ГУДРАТЯН
«__30__» _____ 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи

_____ Віктор ОСТРОВЕРХОВ
«__30__» _____ 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Захист інформації в комп'ютерних системах і мережах»

ступінь вищої освіти – **бакалавр**

галузь знань - 12 Інформаційні технології

спеціальність - 123 Комп'ютерна інженерія

освітньо-професійна програма- «Комп'ютерна інженерія»

Кафедра фундаментальних дисциплін

Форма навчання	Курс	Семестр	Лекції (год.)	Лабораторні (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ.(год.)	Разом (год.)	Екз. (сем.)
Заочна	3	6	8	4	-	-	138	150	6

Єреван- ЄННІ ЗУНУ – 2024

Робоча програма складена на основі освітньо-професійної програми «Комп'ютерна інженерія» підготовки здобувачів вищої освіти на першому (бакалаврському) рівні за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології, затвердженої Вченою радою ЗУНУ (протокол № 9 від 15.06.2022р.), зі змінами відповідно до рішення Вченої ради ЗУНУ (протокол № 11 від 26.06.2024р.).

Робочу програму розробив доктор технічних наук професор, професор кафедри фундаментальних дисциплін Гамлет АРУТЮНЯН.

Робоча програма затверджена на засіданні кафедри фундаментальних дисциплін, протокол № 1 від 27.08.2024 року.

Завідувач кафедри
фундаментальних дисциплін,
доктор технічних наук, професор Гамлет АРУТЮНЯН

Розглянуто та схвалено групою забезпечення спеціальності 123 «Комп'ютерна інженерія», протокол № 1 від 30.08.2024 р.

Голова ГЗС,
д.т.н., професор Гамлет АРУТЮНЯН

Гарант
д.т.н., професор Гамлет АРУТЮНЯН

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
"ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ"

1. Опис дисципліни "Захист інформації в комп'ютерних системах і мережах"

Дисципліна – «Захист інформації в комп'ютерних системах і мережах»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – 12 „Інформаційні технології"	Статус дисципліни – обов'язкова Мова навчання – українська, вірменська
	Спеціальність – 123 „Комп'ютерна інженерія"	Рік підготовки: 3 Семестр: 6
Кількість змістових модулів – 4	Ступінь вищої освіти - бакалавр	Лекції: 8 год. Лабораторні заняття: 4 год.
Загальна кількість годин – 150 год.		Самостійна робота: 138 год.
		Вид підсумкового контролю –екзамен

2. Мета й завдання вивчення дисципліни "Захист інформації в комп’ютерних системах і мережах"

2.1. Мета вивчення дисципліни

Програма та тематичний план дисципліни орієнтовані на отримання студентами навиків та знань щодо захисту інформації.

Студенти вивчають основи використання прикладного програмного забезпечення, яке використовується при захисті інформації, включаючи ознайомлення з вірусами та антивірусними програмами, методи ідентифікації та аутентифікації особи.

2.2 Завдання вивчення дисципліни

Завдання курсу полягає в ознайомленні студентів з основами побудови та використання систем захисту інформації в комп’ютерних системах, а також прищеплення практичних навиків роботи з існуючими сучасними системами захисту інформації, зокрема, криптографічними.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп’ютерної інженерії.

СК4. Здатність забезпечувати захист інформації, що обробляється в комп’ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації

2.4 Передумови для вивчення дисципліни

Зазначена дисципліна включена до циклу дисциплін професійної підготовки за переліком програми. У структурно-логічній схемі навчання зазначена дисципліна розміщена на ІІІ-му курсі. Вивчення курсу "Захист інформації в комп’ютерних системах і мережах" передбачає наявність систематичних та ґрунтовних знань із дисциплін «Комп’ютерні системи», «Комп'ютерні мережі», цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та лабораторних заняттях, самостійної роботи.

2.5. Результати навчання.

В результаті вивчення дисципліни студенти повинні:

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПРН4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

ПРН14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

ПРН19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

ПРН20.Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

ПРН21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

3. Програма навчальної дисципліни "Захист інформації в комп'ютерних системах і мережах"

Змістовий модуль 1. Основи систем захисту інформації у КС Тема 1. Вступ. Поняття захисту інформації.

Інформаційна безпека комп'ютерних систем. Вразливість комп'ютерних систем. Канали витоку інформації, атака та вторгнення в КС. Класифікація загроз безпеці інформації та інформаційним системам. Перехват, переривання. Модифікація та фальсифікація. Радіотехнічне, організаційне, комунікаційне, програмно-технічне.

Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні.

Політика безпеки. Нормативно-правове та організаційне забезпечення безпеки. Комунікаційно-технічне забезпечення. Програмне забезпечення.

Змістовий модуль 2. Управління доступом та розмежування прав доступу до інформації

Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів.

Етапи ідентифікації, авторизації та автентифікації користувачів Прості паролі. Способи формування та реєстрації паролів. «Слабкі» паролі. Характеристики парольного захисту.

Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.

Паролі одноразові, ідентифікатори, секретні функції, процедури «рукостискання». Списки доступу, мандатні списки. Механізми розширення прав доступу. Принцип мінімальних привілей.

Змістовий модуль 3. Атаки на системи захисту інформації та методи захисту від них.

Тема 5. Основні типи атак та методи захисту від них.

Модель системи захисту Adept-50. Типи об'єктів та категорій. Модель простору безпеки Хартсона. Домени повноважень користувачів.

Тема 6. Канали витоку інформації. Сучасні атаки на реалізацію та відповідні методи протидії.

Модель системи захисту Бела і Лападули. Матриця прав доступу. Потоки запитів суб'єктів до об'єктів. Модель моніторингу безпеки. Лічильники небезпечних подій. Вектор індикації аномалій в діях користувачів.

Змістовий модуль 4. Захист інформації в комп'ютерних системах.

Тема 7. Найпростіші шифри.

Перестановки та підстановки. Шифри «Скітала», Полібія, Цезаря. Шифри Плейфера, Уітстона. Шифрувальні таблиці. Роторні машини. Маскування. Шифр Вернама.

Тема 8. Симетричні криптоалгоритми.

Система Люцифер. Стандарт DES. Функція шифрування та управління ключами. Режими ECB,CBC,OFB,CFB.

Тема 9. Асиметричні криптоалгоритми.

Алгоритм асиметричного шифрування інформації. Алгоритм Діффі-Хелмана. Алгоритм Ель-Гамаля.

Тема 10. Електронний цифровий підпис.

Алгоритми цифрового підпису Blowfish, RC-5, CAST-128. Хеш-згортка повідомлень. Алгоритми MD-5, SHA, ГОСТ 34.11-94.

Змістовий модуль 5. Захист інформації в комп'ютерних мережах.

Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.

Особливості Wi-Fi мереж. Основні атаки в Wi-Fi мережах та методи захисту від них. Захист мобільного зв'язку.

Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.

Поняття інтернет-банкінгу. Апаратні засоби здійснення платежів та методи їх захисту. Захист особистих фінансових даних.

4. Структура залікового кредиту дисципліни "Захист інформації в комп'ютерних системах мережах"

(заочна форма навчання)

	Кількість годин		
	Лекції	Лабораторні заняття	Самостійна робота
Змістовий модуль 1			
Тема 1. Вступ. Поняття захисту інформації.			10
Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні	1	1	10
Змістовий модуль 2			
Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів..		1	10
Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.	1		10

Змістовий модуль 3			
Тема 5. Основні типи атак та методи захисту від них	1		10
Тема 6. Канали витоку інформації.			10
Тема 7. Захист інформації в комп'ютерних системах..	1		10
Тема 8. Симетричні криптоалгоритми.	1	1	10
Тема 9. Асиметричні крипто алгоритми.	1	1	10
Тема 10. Електронний цифровий підпис.	1		10
Змістовий модуль 4			
Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.	1		15
Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.			18
Разом	**8**	**4**	**138**

5. Тематика лабораторних занять

Лабораторна робота №1.

Тема: Шифрування файлів та папок засобами Secure IT.

Мета: Вивчити засіб захисту інформації Secure IT.

Питання для обговорення:

1. Методи шифрування
2. Парольний захист.
3. Процедура дешифрування.

Лабораторна робота №2.
Тема: Захист текстових документів в Microsoft Word.
Мета: Навчитися захищати документ засобами Microsoft Word.
Питання для обговорення:
1. Методи захисту.
2. Простий пароль.
3. Модифікація прав доступу.

Лабораторна робота №3.
Тема: Захист інформації засобами ОС Windows.
Мета: Навчитися захищати інформацію засобами ОС Windows.
Питання для обговорення: 1.
Технологія BitLocker.
2. Технологія AppLocker.
3. Батьківський контроль.

Лабораторна робота №4.
Тема: Захист інформації за допомогою антивірусних програм.
Мета: Вивчити можливості сучасних антивірусних програм.
Питання для обговорення:
1. Антивірусні програми.
2. Функції мережевого екрана.
3. Журнал активності.

Лабораторна робота №5.
Тема: Розробка та дослідження засобів ідентифікації користувачів в комп'ютерних системах.
Мета: Навчитися здійснювати ідентифікацію користувачів комп'ютерних систем.
Питання для обговорення:
1. Процедура ідентифікації.
2. Методи ідентифікації.
3. Рівні захисту КС.

Лабораторна робота №6.

Тема: Розробка та дослідження засобів аутентифікації користувачів в комп'ютерних системах.

Мета: Навчитися здійснювати аутентифікацію користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура аутентифікації.
2. Методи аутентифікації.
3. Процедура авторизації.

Лабораторна робота №7.

Тема: Дослідження засобів створення та використання електронних цифрових підписів користувачів в комп'ютерних системах.

Мета: Навчитися створювати та застосовувати електронний підпис користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура аутентифікації.
2. Методи аутентифікації.
3. Процедура авторизації.

7. Самостійна робота студентів

(заочна форма навчання)

№ п/п	Тематика
1	Законодавчі аспекти захисту інформації.
2	Основні загрози безпеки інформації. Забезпечення безпеки інформації в комп'ютерних системах і мережах.
3	Проблема ідентифікації користувача та механізми підтвердження його істинності.
4	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
5	Проблема ідентифікації користувача та механізми підтвердження його істинності.
6	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
7	Взаємна перевірка істинності користувачів.
8	Біометрична ідентифікація особи.
9	Електронний цифровий підпис.
10	Вітчизняні стандарти електронного цифрового підпису.

8. Засоби оцінювання та методи демонстрування результатів навчання

У навчальному процесі застосовуються: лекції, в тому числі з використанням мультимедіапроектора та інших ТЗН; практичні заняття; самостійна робота студента, робота в Інтернет.

У процесі вивчення дисципліни "Захист інформації в комп’ютерних системах" використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточні опитування;
- презентації результатів виконання завдань та досліджень;
- оцінювання результатів самостійної роботи студентів;
- екзамен.

10. Критерії, форми поточного та підсумкового контролю

В процесі вивчення дисципліни "Захист інформації в комп’ютерних системах" використовуються наступні методи оцінювання навчальної роботи студента:

- поточне тестування та опитування;
- оцінювання наскрізного проекту у результаті самостійної роботи;
- підсумковий екзамен.

Оцінювання здійснюється за 100 бальною шкалою.

Критерії оцінювання знань:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст питань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без

аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1–59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань.

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90-100	Відмінно	A (відмінно)
85-89	Добре	B (дуже добре)
75-84		C (добре)
65-74	Задовільно	D (задовільно)
60-64		E (достатньо)
35-59	Незадовільно	FX (незадовільно, з можливістю повторного складання)
1-34		F (незадовільно, з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Антивірусні програми, фаєрволи	5, 6
2.	Операційні системи	3, 4, 6
3.	Secure IT	8, 9
4.	Java, C++, Python Trial Version	10-12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах. К.: КМ Академія, 2006. 244 с.

2. Бабак В.П. Теоретичні основи захисту інформації. Підручник. НАУ, 2008.752 с. 3. Вакалюк Т.А. Захист інформації в комп'ютерних системах. Навчально-методичний посібник. Житомир: Вид-во ЖДУ, 2013.136 с.

4. Вербіцький О.В. Вступ до криптології. Львів: Видавництво НТЛ., 2008, 248 с. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах. Ужгород: УжНУ, 2021 184 с.

5. Грайворонський М. В., Новіков ОМ. Безпека інформаційно-комунікаційних систем. К.: Видавнича група BHV, 2009. 608 с. 7. Гребенюк А.М. Управління інформаційною безпекою: конс. лекцій. ДніпроЖ: ДДУВС ,2019. 68 с. 8. Державна служба спеціального зв'язку та захисту інформації України: веб-сайт. URL: https://cip.gov.ua/ua/news (дата звернення 25.08.2022).

9. Захарченко М. В., Онацький О. В., Йона Л. Г., Шинкарчук Т. М. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. Одеса: ОНАЗ ім. О. С. Попова, 2011. 184 с.

10. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 218 с.

11. Нормативно-правове забезпечення інформаційної безпеки: Збірник нормативно-правових до кументів / Уклад. О.Г. Корченко, Ю.О. Дрейс. Житомир : ЖВІ НАУ, 2018. 280 с.

12. Остапов С. Е., Валь Л.О. Основи криптографії: навчальний посібник. Чернівці: Книги–XXI, 2008. 188 с.

13. Остапов С. Е., С. П. Євсеєв С. П., Король О. Г. Технології захисту інформації: навчальний посібник. Х. : Вид. ХНЕУ, 2016. 476 с.

14. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп'ютерних системах та мережах : навч. посіб. Х.: НТУ «ХПІ», 2014. 251 с.

15. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: Підручник. К. : НАУ, 2016. 620 с.

16. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. К. : Вид-во DIRECTLINE, 2019. 714 с.

17. Binance academy: веб-сайт. URL: https://academy.binance.com/uk (дата звернення 22. 08. 2022).